Personnel and Administrative Policy and Procedure

SUBJECT: Information Technology Resources	**EFFECTIVE DATE:** June 1, 2006 **REVIEWED:** **REVISED:** May 15, 2006; December 2012
CATEGORY: 500 **POLICY NUMBER: 500.1**	**CROSS REFERENCE:** Internet Usage Policy 500.2 Electronic Mail Policy 200.14

Purpose: To ensure the appropriate, cost effective, and efficient use and operation of the City's computing environment through local and wide area networks and Internet connectivity.

Definitions
City: The local government agency known as the City of Milwaukie.
User: All persons accessing the City's network and computing resources, whether authorized or not, including its employees, volunteers, City Council, and contractors.
Strong Passwords: Passwords that contain combinations of uppercase and lowercase letters, numbers and special characters. (e.g. Pa$$w0Rd2)
Sensitive Information: Personal, confidential, or protected information whose release is unauthorized.
Downloading - Moving a computer file from a host machine to the local machine (e.g. server, website host machine, ftp server, etc.)
Uploading - Moving a computer file from the local machines to a host machine.
Profile – Set of computer files that define the user's local computer settings (e.g. printer selections, color sets, application settings, etc.)
Removable Media – includes, but is not limited to, computing devices that store or transfer data such as, floppy disks, CDs, DVDs, USB devices (e.g. jump drives, thumb drives, flash drives, etc.), zip disks, memory sticks, secure cards, PDAs (personal digital assistants), etc.
Computer locking – Putting the computer in a secure state where no one else can view or manipulate the applications and/or files on a computer. Only the user locking the computer or a network administrator can release the lock on a computer.
Bandwidth – Data transfer rate or the amount of data that can be carried from one point to another point in a given time frame (usually measured in kilobits or megabits per seconds) via a dedicated communication channel. (Example: T-1 line has a bandwidth of 1.54 Mbps or 1.54 megabits per second.)
Turnkey system – Usually refers to a vertical hardware, software and application computer system purchased, configured and maintained by a vendor or outside agency for a specific task.
Untrusted source – A person or group with whom you are NOT actively conducting business across an electronic medium.

Scope: All users

Policy

1. **Computers – Specification and Acquisition**
   1.1. *Computer Equipment Specification* - The Information Systems and Technology Department (IST) will specify the generic desktop computer, laptop and software used by staff within the City. Individual departments are responsible for identifying and communicating special computing

needs within their department to IST for proper specification and eventual purchase. Some standalone systems within the City may be the entire responsibility of the individual department as they are turnkey systems provided by a vendor for a specific purpose and wholly supported by the vendor. Any turnkey system requiring network connectivity will require consultation and approval by IST prior to hook-up.

1.2. *Computer Equipment* Acquisition - All networked computers and related devices will be purchased and maintained by the Information Systems and Technology Department (IST). The IST Department will follow all established purchasing rules in the procurement of all computer and peripheral equipment. Purchase orders and credit card orders for equipment will be completed by the IST Department with sign-off by the individual department manager, if necessary. No purchase order for computer equipment, peripherals and software will be released by Finance unless it has the IST Director's approval.

1.3. *Computer Equipment Funding* - The City has established a Computer Reserve Fund to capture computer, laptop, printer and server replacement dollars. Each department contributes annually to the fund based on the number of desktop computers and laptops in use by the department. Each department also pays a proportionate share of the projected server and printer replacement costs identified by the IST Department. The IST Department will make replacement purchases of equipment using these funds as necessary throughout the year.

2. **Computer – System Integrity and Security**

2.1. *Resource Accessibility* - Access to the City's network, computers, Geographic Information Systems (GIS) and telecommunications systems is restricted to authorized personnel. Access will be limited to authorized personnel through the use of passwords, user identification codes, terminal locks or locked entry doors. Access and movement of all personnel who are not authorized employees of the City will be monitored.

Remote access to the City's network is available for those employees whose job requires it. Questions on remote access should be directed to either the IST Director or HR Director.

Access to IST computer server and telecommunications rooms is restricted to authorized personnel. Entry to these controlled areas requires an IST or authorized personnel escort.

2.2. *Network Usage* - Networking is a communication system that allows computers to exchange information between themselves and fixed storage objects (servers), shared peripheral devices, such as printers, and other devices on local area networks (LAN). Computers can also access and communicate with hosts and devices across a wide area network (WAN) or on the Internet. Network usage is available to all employees seven days a week twenty-four hours a day.

Streaming audio or video, such as radio stations or music videos, to local computers for personal use is prohibited as it utilizes a large portion of available bandwidth. The bandwidth of the Internet line is shared between all City staff, business-oriented Internet traffic (e-mail processing, web browsing, etc.) public access to the City's Internet website and staff of Oak Lodge Sanitary District. Streaming audio and/or video for business purposes (web casts, webinars, approved online training, etc.) is allowed.

To accommodate the computing needs of the City, the IST Department will provide advanced outage notifications in the event of any planned shared device down time. Advanced notification may not be available in the event of an emergency.

2.3. *Passwords* - Properly implemented and administered, user passwords improve the likelihood that users are whom they profess to be and user access can be controlled effectively.

User passwords are authenticated by the system before the user is granted access to network resources. A user's authorization shall be removed when the user's employment is terminated or the user transfers to a position where access is no longer required.

Users shall not share their password with another user. In addition, users shall not access any network resources with another user's password. Each user is responsible for any unauthorized use of their password. Users requiring access to the network or any network resources should notify their supervisor to have a request for access submitted to the IST Helpdesk.

Users will contact the Helpdesk if they have forgotten their password or believe their password has been compromised. IST support personnel will reset the password and ensure the user can log back onto the network or affected application.

User network passwords will change every ninety (90) days to maintain an effective deterrent against unauthorized access and use. When changing passwords, the use of family member names; social security numbers, or anything that can be easily guessed or directly associated with the user, should be avoided. Users are encouraged to use strong network passwords. (The upcoming implementation of the Windows Server 2003 operating system will require strong passwords.)

Password protected screen savers hinder IST support personnel's access to the system. Staff is encouraged <u>not</u> to use local passwords. If used, access to the system must be provided in order to receive assistance.

2.4. *Securing the Computer* - Users are responsible for properly securing access to their computer systems. This includes access to all network and application resources.

Users will lock their computer systems when they temporarily step away from their desk and cannot actively monitor their workstation. Users will properly log out of their computers when they leave the building or no longer require access to the network. This will free up a computer resource for other staff, especially in shared computer work environments. It also ensures the security of your account from possible security breaches.

Users should save all open work before locking their workstations. This will assist in protecting the data should IST personnel need to administratively break through a computer lock forcing a log off of the user account. IST personnel will not be held responsible for lost data resulting from unsaved files when breaking through a computer lock for business purposes.

2.5. *Anti-Virus Protection* - Computers are highly susceptible to infection by viruses that can damage system operability or cause data loss. Viruses are computer programs that are written specifically to cause damage to a recipient machine or machines if the infected computer is part of a network. Viruses can enter the machine several ways; through infected e-mail, infected files on a floppy or USB device, Internet file downloads, etc. IST requires each computer capable of being infected by a virus to be loaded with an approved anti-virus application prior to placement on the network.

Users can assist in the prevention and detection of viruses on the computer by adhering to these guidelines:

- Do not use or load any software on the computer,
- Do not open any e-mail with an attachment that is from an untrusted source;
- Do not engage in intentionally spreading computer viruses (legal action will be taken against anyone caught intentionally spreading viruses);
- Do not use a computer suspected of containing a virus, contact the Helpdesk immediately.

2.6. *Downloading, Uploading and Copying Files* - Downloading and uploading files between the local City computer and City servers are permitted to perform the duties of one's job. Users shall not upload or download files that contain known viruses or do not contain information relating to the business of the City (personal files). Users, excluding Police Department personnel when business necessity dictates, shall not knowingly upload, download or store any files containing pornographic or sexually explicit material on the City's computer systems. Police Department personnel investigating sexually oriented crimes must store any case-related pornographic or sexually explicit material on a network resource accessible only to the Police Department and IST personnel.

Users shall not download installation or executable files from the Internet or any other source. Users should only knowingly download files for viewing information, such as Adobe PDF documents or Microsoft Word, Excel or PowerPoint files that contain relevant information about the business of the City. Users shall not download files of a personal nature, such as audio, video and graphics files. These files are usually quite large, use a significant amount of bandwidth and resources to download and view, and occupy valuable server space reserved for business related information.

Users shall not upload or e-mail files of a sensitive nature to an unsecured location on the network or to any host machine outside the City's network without proper approval from a department director. Users shall not upload or e-mail any program files or sensitive data to hosts or accounts outside the City's network without proper authorization.

Users should use discretion in copying files. Data should never be <u>removed</u> from the network to portable devices, such as floppy, jump drive, CD or DVD. Data should be <u>copied</u> to a removable device <u>when</u> <u>required</u> leaving an exact copy on the network where it can be accessed in the event of media failure and backed up for safekeeping. Copying data to personal media is prohibited. Copying data to media or e-mailing data to a personal e-mail account to work on non-City computers is highly discouraged.

2.7. *Data Storage* - Data should be stored on a network resource and not on the local computer system. Network servers are backed up and tapes stored in a fireproof location for safekeeping for a specified retention period. Data stored on the local computer system is not backed up, thereby putting it at risk for permanent loss. Data should never be stored on the desktop of the local computer or in the folder labeled "profile." If a user profile corrupts the data associated with the profile directory will be lost.

2.8. *Data Sharing* - Data shared between employees should be stored on a network server. Proper directory level security should be applied to the data to ensure confidentiality and user's ability to manipulate the data. Please contact the Helpdesk for assistance in creating and/or applying directory permissions.

Data shared with consultants, vendors, partner agencies and other business associates should be protected through the use of a non-disclosure statement either contained within a contract or as an attachment, especially when data is of a sensitive nature. Data should not be shared with outside sources without express permission or knowledge of a department director or the City Manager. Some data used by City staff is protected by contracts with partner agencies, which expressly prohibit the release of information to a third party.

Data released to the general public shall follow the policies and procedures adopted by the City as pursuant to ORS 192.410 and 192.505.

2.9. *Backups and Restores* - The IST Department shall backup and store critical network computer data files used by staff at least once each business day. These backups shall be stored in a fireproof place according to a pre-established retention schedule. Backups and data retention schedules shall adhere to Oregon's General Records Retention Schedules (OAR 166-200).

IST will perform any required restores of missing or corrupt files and applications providing the data is available as outlined in the retention period of the backup tapes.

3. Computer – Hardware

3.1. *Installation and Maintenance* - The IST Department has the primary charge to install and maintain all computer equipment in the City. Staff requiring upgrades to their current computer equipment or maintenance on their computer equipment should contact the City's Helpdesk for assistance. Staff should not attempt to "fix" their own computer equipment.

Requests for new equipment should be submitted to the IST Director along with an explanation of the intended use of the equipment, software licensing issues and budgetary information for the acquisition of the proposed equipment.

3.2. *Computer Relocation* - The IST Department will arrange for the relocation of any supported computer system in the City. Departments or staff requiring a move of their computing system(s) will contact the City's Helpdesk to make proper arrangements for the relocation of all affected computer equipment. Adequate and reasonable notification must be given in all proposed moves in order to accommodate proper scheduling of staff and required resources. Staff will not attempt to relocate computer equipment themselves.

3.3. *Removable Media* - Users will use only City provided and approved removable media devices to transport City data. All removable devices requiring software installations will be approved and installed by the IST Department. Users will not use or transfer City data to personal removable media devices.

3.4. *Personal Equipment* - The IST Department will not install personal or City-owned software, configure or perform maintenance on any personal computing equipment. Personal computing equipment is not allowed on the City's network. City data will not be transferred to or from personal computing equipment. Departmental mobile computing devices may be available if staff needs to work remotely.

4. Computer – Software

4.1. *Installation of Software* - The IST department and authorized vendors and/or contractors working with the IST department are the only staff to install any and all software on City computers, servers, networking equipment and other computing devices.

The IST Department will not install any game software on the City computers. Users are not to download, access, install, store or play any games on the City computers. Any form of game playing is prohibited on City computers.

Users shall not attempt to download or install any software from the Internet to their computer without prior written approval of the IST Director. This restriction includes "freeware" or "shareware," available on the Internet at no or low cost for limited use. If you suspect a file may have accidentally been downloaded to your computer, contact IST immediately for inspection and removal.

The City of Milwaukie's Ledding Library may purchase, store and lend to patrons only such software that is clearly marked "For Ledding Library Patron Use Only" and meets the full copyright compliance as specified in Copyright Law Title 17, Chapter 1, Section 109(b). Software designated "For Ledding Library Patron Use Only" shall not be used on any internal computing system of the City of Milwaukie. A test computer may be placed at the Ledding Library for the purposes of installing and evaluating new patron software. This test system will be given its own unique logon access and is not intended for general staff use.

4.2. *Software Licenses* - Users may not knowingly use software for which the City lacks the appropriate license. Users should notify their supervisor or the IST Director if they are aware of the use or distribution of unauthorized software in the City. Users may not loan or give to anyone software licensed to the City.

The IST Department must (1) establish and maintain a record keeping system for software licenses, hardware, original CD-ROMs and diskettes, user information, and review information in compliance with OAR 166-200-0060; (2) maintain this information in a secure, central location; and (3) consider the use of software management programs to automate such record keeping.

4.3. *City Standard Software* - Standard software packages for the City are those that have been evaluated and purchased by the City for general use on City computers. Support for these packages can be obtained from the Helpdesk.

Specialized software packages are those other than the standard City software that may be required to perform special functions not available through one of the standard software packages. IST support personnel will provide installation and configuration support for these packages, either through direct support from the Helpdesk or through a software maintenance contract with the software vendor. Application usage support for specialized applications may not be available from the Helpdesk.

4.4. *Requests for New Software* - All new requests for software packages will be processed through the IST Director. Users requesting new software should submit a formal request, which contains the following:

- Reason new package is required and why existing software packages are not effective,
- Name of software package and vendor or retailer where IST can obtain further information
- Specify who will use the package and how it will be used within the City,
- Budgetary information (budgeted or unbudgeted item), and
- Brief description of the capabilities of the new package.

4.5. *Software Upgrades* - Software upgrades of City standard packages will be tested, purchased and implemented by the IST department. All previous releases of software must be removed when upgrades are made, and all previous versions must be erased from the local computer according to copyright laws.

Software upgrades of specialized software packages will be tested and implemented by the IST department or the associated vendor/retailer. Individual departments are responsible for purchasing the upgrades to specialized software through the IST Department unless the upgrade is covered in an annual maintenance agreement where upgrades are part of the contract.

4.6. *Disposition of Old Software* - Software is usually not a transferable asset and cannot be resold. Departments are responsible for notifying the IST department of the intended retirement of an application. Notification should include the name, version number, manufacturer and serial number of the package to be removed. Once received the IST department will decide if the package should be archived or properly destroyed.

4.7. *Personal Software* - Employees, City Council and Other City Personnel may not use or distribute personally owned software on the organization's computers or networks. Such software threatens the integrity and security of the City's computers and networks. It may also violate copyright laws.

5. Support and Training

5.1. *Help Desk* - The City has a centralized contact area within IST for addressing all computer, application, voice and network problems and requests.

5.2. *Contact Information* - Staff can reach the Help Desk by dialing 7407 internally or 503-786-7407 outside the organization for assistance. If you reach voicemail when dialing the Help Desk number please be sure to leave your name, a number where you can be reached and detailed message. The Help Desk support team will be paged by the voicemail system.

You can also reach the Help Desk via e-mail by choosing the distribution list from the global address book within Outlook or by using the helpdesk@ci.milwaukie.or.us from outside the City's e-mail system. E-mail is the preferred method of communication for the Help Desk as several IST staff monitor the Help Desk e-mail communications.

5.3. *Hours of Operation* - The Help Desk is staffed during normal business hours, Monday through Friday from 8:00 a.m. to 5:00 p.m. Staff needing emergency assistance after working hours should contact 503-786-7500 (non-emergency line at Lake Oswego Communication Center - LOCOM) and request someone in IST be paged. The IST Department carries cell phones in order to respond to any emergencies.

5.4. *Response Times* - Every effort will be made to evaluate and address each request submitted to the Help Desk within 24 hours. Actual problem resolution and service order requests may take longer than 24 hours to complete depending on the nature of the problem or request and availability of staff.

5.5. *Response Methods* - IST Department staff may remotely or directly connect to staff computers for the purposes of assisting in troubleshooting and/or correcting a reported problem.

IST Department staff may also remotely or directly connect to staff computers for the purposes or applying operating system or application patches and upgrades. The IST Department will make every effort to notify affected staff prior to applying any upgrades or patches.

IST Department staff may also troubleshoot and/or solve problems with users via e-mail or the telephone

5.6. *IST Provided Training – Internal and External* - The IST Department will provide in-house user training as new technologies and concepts are introduced across the organization.

IST may also arrange for outside instruction in certain situations where a small group of users require training on a specific application.

One-on-one training is also available from IST staff as applicable.

Guidelines for Use

Responsibilities

All Users: Users shall read and comply with all aspects of the aforementioned policy. Users are responsible for notifying the IST Director or Human Resources Director of any violations to this policy.

Users shall safeguard all computing hardware, software, licenses and data entrusted to them as part of their employment with the City.

As part of the City's software management process, the IST Department shall conduct periodic, random reviews of all City computers and networks to determine the software resident on such systems and whether the City has the appropriate licenses for all such software. Staff may be held responsible for the existence of any software on local computers for which the City lacks the appropriate licenses.

All City of Milwaukie Department Managers

1. Managers are responsible for ensuring that **all** their employees have signed an Information Technology Resources Policy Agreement and that it is placed in the employee's personnel file.

2. Managers and Supervisors, in cooperation with the Human Resources Director, are responsible for monitoring computer usage and taking appropriate action when this policy is contravened.

Violations of any portion of this policy will be cause for disciplinary action up to and including termination.

Complete and Return to HR

INFORMATION TECHNOLOGY RESOURCE AGREEMENT

I, ____, have received, read,
(Print Name)

understand and agree to comply with the provisions and terms of the Information Technology Resource Policy.

____
Employee Signature

____
Date